WILLIAM L. ANTHONY (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
MARK R. WEINSTEIN (State Bar No. 193043)
ORRICK, HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

STEVEN ALEXANDER (admitted *Pro Hac Vice*)
KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
JAMES E. GERINGER (admitted *Pro Hac Vice*)
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

Attorneys for Defendant and Counterclaimant,
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant.	CASE NO. C01-1640 SBA **MICROSOFT CORPORATION'S PATENT LOCAL RULE 4-1(a) STATEMENT (LIMITED TO "MINI-MARKMAN" CLAIMS)**
MICROSOFT CORPORATION, a Washington corporation, Counterclaimant, v. INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Counter Claim-Defendant.	

Pursuant to Patent Local Rule 4-1(a), Microsoft submits below the claim terms, phrases, and clauses of the twelve selected "Mini-Markman" patent claims that Microsoft presently submits, subject to discussions with InterTrust, should be construed by the Court, in addition to construing each claim as a whole.

Set forth in Section A, below, is a list of individual claim terms that Microsoft presently submits, subject to discussions with InterTrust, should be construed by the Court. Individual claim terms should be construed wherever they are found in these twelve claims.

Set forth in Section B, below, are the phrases and clauses that Microsoft presently submits, subject to discussions with InterTrust, should be construed by the Court. The claim phrases and clauses that Microsoft presently submits, subject to discussions with InterTrust, should be governed by 35 U.S.C. § 112(6), are identified in Section B by double underlining.

Many of these claim terms, phrases and clauses are indefinite and otherwise improper under 35 U.S.C. § 112(2), and Microsoft reserves all rights to assert those defects as to each of these claim terms, phrases and clauses.

The grouping of individual claim terms below is for convenience only and does not imply any particular connection, or lack of connection, between any terms.

A. Individual Claim Terms

- a digital file, digital file
- access, accessed, access to, accessing
- addressing
- allowing, allows
- applying . . . in combination
- arrangement
- aspect
- associated with
- authentication
- authorization information, authorized, not authorized
- budget control, budget

- can be
- capacity
- clearinghouse
- compares, comparison
- component assembly
- contain, contained, containing
- control (n.), controls (n.)
- controlling, control (v.)
- copied file
- copy, copied, copying
- copy control
- creating, creation
- data item
- derive, derives
- descriptive data structure
- designating
- device class
- digital signature, digitally signing
- entity, entity's control
- environment
- executable programming, executable
- execution space, execution space identifier
- generating
- govern, governed, governed item, governing
- halting
- host processing environment
- identifier, identify, identifying
- including
- information previously stored
- integrity programming
- key
- load module
- machine check programming
- metadata information
- opening secure containers
- operating environment, said operating environment
- organization, organization information, organize
- portion
- prevents
- processing environment

- protected processing environment
- protecting
- record
- required
- resource processed
- rule
- secure
- secure container, secure containers
- secure container governed item
- secure container rule
- secure database
- secure execution space
- secure memory, memory
- secure operating environment, said operating environment
- securely applying
- securely assembling
- securely processing
- securely receiving, securely receiving . . . a control
- security
- security level, level of security
- specific information, specified information
- tamper resistance
- tamper resistant barrier
- tamper resistant software
- tampering
- use
- validity
- virtual distribution environment

B. Claim Phrases and Clauses

'193:1

- receiving a digital file including music
- a budget specifying the number of copies which can be made of said digital file
- controlling the copies made of said digital file
- determining whether said digital file may be copied and stored on a second device based on at least said copy control
- if said copy control allows at least a portion of said digital file to be copied and stored on a second device
- copying at least a portion of said digital file

- transferring at least a portion of said digital file to a second device
- storing said digital file

'193:11

- receiving a digital file
- determining whether said digital file may be copied and stored on a second device based on said first control
- identifying said second device
- whether said first control allows transfer of said copied file to said second device
- said determination based at least in part on the features present at the device
- if said first control allows at least a portion of said digital file to be copied and stored on a second device
- copying at least a portion of said digital file
- transferring at least a portion of said digital file to a second device
- storing said digital file

'193:15

- receiving a digital file
- an authentication step comprising:
- accessing at least one identifier associated with a first device or with a user of said first device
- determining whether said identifier is associated with a device and/or user authorized to store said digital file
- storing said digital file in a first secure memory of said first device, but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized
- storing information associated with said digital file in a secure database stored on said first device, said information including at least one control
- determining whether said digital file may be copied and stored on a second device based on said at least one control
- if said at least one control allows at least a portion of said digital file to be copied and stored on a second device,
- copying at least a portion of said digital file
- transferring at least a portion of said digital file to a second device
- storing said digital file

'193:19

- receiving a digital file at a first device
- establishing communication between said first device and a clearinghouse located at a location remote from said first device
- using said authorization information to gain access to or make at least one use of said first digital file
- including using said key to decrypt at least a portion of said first digital file

- receiving a first control from said clearinghouse at said first device
- storing said first digital file in a memory of said first device
- using said first control to determine whether said first digital file may be copied and stored on a second device
- if said first control allows at least a portion of said first digital file to be copied and stored on a second device
- copying at least a portion of said first digital file
- transferring at least a portion of said first digital file to a second device including a memory and an audio and/or video output
- storing said first digital file portion

'683:2

- user controls
- the first secure container having been received from a second apparatus
- an aspect of access to or use of
- the first secure container rule having been received from a third apparatus different from said second apparatus
- hardware or software used for receiving and opening secure containers
- said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers
- protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus
- hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container
- hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.

'721:1

- digitally signing a first load module with a first digital signature designating the first load module for use by a first device class
- digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class
- distributing the first load module for use by at least one device in the first device class
- distributing the second load module for use by at least one device in the second device class

'721:34

- arrangement within the first tamper resistant barrier
- prevents the first secure execution space from executing the same executable accessed by a second secure execution space having a second tamper resistant barrier with a second security level different from the first security level

'861:58

- creating a first secure container
- including or addressing . . . organization information . . . desired organization . . . and metadata information at least in part specifying at least one step required or desired in creation of said first secure container
- at least in part determine specific information required to be included in said first secure container contents
- rule designed to control at least one aspect of access to or use of at least a portion of said first secure container contents

'891:1

- resource processed in a secure operating environment at a first appliance
- securely receiving a first entity's control at said first appliance
- securely receiving a second entity's control at said first appliance
- securely processing a data item at said first appliance, using at least one resource
- securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item

'900:155

- first host processing environment comprising
- said mass storage storing tamper resistant software
- designed to be loaded into said main memory and executed by said central processing unit
- said tamper resistant software comprising: . . . one or more storage locations storing said information
- derives information from one or more aspects of said host processing environment,
- one or more storage locations storing said information
- information previously stored in said one or more storage locations
- generates an indication based on the result of said comparison
- programming which takes one or more actions based on the state of said indication
- at least temporarily halting further processing

'912:8

- identifying at least one aspect of an execution space
- required for use and/or execution of the load module
- said execution space identifier provides the capability for distinguishing between execution spaces providing a higher level of security and execution spaces providing a lower level of security
- checking said record for validity prior to performing said executing step

'912:35

- received in a secure container
- said component assembly allowing access to or use of specified information
- said first component assembly specified by said first record

Dated: November 8, 2002

By: _____

WILLIAM L. ANTHONY
ERIC L. WESENBERG
MARK R. WEINSTEIN
ORRICK HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400

STEVEN ALEXANDER
KRISTIN L. CLEVELAND
JAMES E. GERINGER
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391

Attorneys for Defendant
MICROSOFT CORPORATION

Of Counsel:

T. Andrew Culbert, Esq.
One Microsoft Way
Building 8
Redmond, WA 98052-6399
Phone: 425-882-8080

DECLARATION OF SERVICE BY E-MAIL AND FIRST CLASS MAIL

I am more than eighteen years old and not a party to this action. My place of employment and business address is 121 S.W. Salmon St., Suite 1600, Portland, OR 97204.

On November 8, 2002, I served on counsel for InterTrust Technologies Corporation:

MICROSOFT CORPORATION'S PATENT LOCAL RULE 4-1(a) STATEMENT by e-mail delivery and by placing true copies of these papers in envelopes addressed to:

Michael H. Page, Esq. John W. Keker, Esq. Jon B. Streeter, Esq. KEKER & VAN NEST, LLP 710 Sansome Street San Francisco, CA 94111 Phone: 415-391-5400 Fax: 415-397-7188 E-mail: mhp@kvn.com	Stephen E. Taylor, Esq. Taylor & Co. Law Offices 1050 Marina Village Parkway Suite 101 Alameda, CA 94501 Phone: 510-865-9401 Fax: 510-865-9408 Email: staylor@tcolaw.com
Steven H. Morrissett, Esq. Finnegan Henderson Farabow Garrett & Dunner Stanford Research Park 700 Hansen Way Palo Alto CA 94304-1016 steven.morrissett@finnegan.com	

and sealing each envelope, affixing adequate first-class postage and depositing it in the U.S. mail at Portland, Oregon.

I declare under penalty of perjury that the foregoing is true and correct. Executed on November 8, 2002, at Portland, Oregon.

Toni R. Lavelle
(SIGNATURE)

Toni R. Lavelle
(PRINT NAME)